

On Galois Representations of Weight One

Gabor Wiese

12th January 2013

Abstract

A two-dimensional Galois representation into the Hecke algebra of Katz modular forms of weight one over a finite field of characteristic p is constructed and is shown to be unramified at p in most cases.

MSC (2010): primary 11F80; secondary 11F33, 11F25.

1 Introduction

Let $g = \sum_{n=1}^{\infty} a_n q^n$ be a holomorphic cuspidal Hecke eigenform of weight 1 on $\Gamma_1(N)$ with Dirichlet character ϵ . Deligne and Serre [DS74] constructed a Galois representation

$$\rho_g : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{C}),$$

which is irreducible, unramified outside N and characterised by $\rho_g(\text{Frob}_\ell)$ having characteristic polynomial $X^2 - a_\ell X + \epsilon(\ell)$ for all primes $\ell \nmid N$. Here, and throughout, Frob_ℓ denotes an arithmetic Frobenius element. Let now $p \nmid N$ be a prime number. Reducing ρ_g modulo (a prime above) p and semisimplifying yields a Galois representation

$$\overline{\rho}_g : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{F}}_p),$$

which is still unramified outside N (in particular, at p) and still satisfies the respective formula for the characteristic polynomials at all unramified primes. In fact, $\overline{\rho}_g$ only depends on the reduction of (the coefficients of) g modulo (a prime above) p .

In this article, we shall work more generally and study normalised cuspidal Katz eigenforms g over $\overline{\mathbb{F}}_p$ of weight 1 on $\Gamma_1(N)$ with Dirichlet character ϵ and q -expansion (at ∞) $\sum_{n=1}^{\infty} a_n q^n$ for $p \nmid N$ (see Section 2). Unlike when the weight is at least 2, not all such g can be obtained by reducing holomorphic weight 1 forms. The first such nonliftable example was found by Mestre (see Appendix A of [Edi06]). Nevertheless, g also has an attached Galois representation $\overline{\rho}_g$ which is unramified outside Np and such that the characteristic polynomials at unramified primes look as before. In their study of companion forms, Gross, Coleman and Voloch proved that $\overline{\rho}_g$ is also unramified at p in almost all cases.

Proposition 1.1 (Gross, Coleman, Voloch). *If $p = 2$, assume that $a_p^2 \neq 4\epsilon(p)$. Then the residual representation $\overline{\rho}_g$ is unramified at p .*

Proof. The case $p > 2$ is treated by [CV92] without any assumption on a_p . [Gro90] proves the result for all p (i.e. including $p = 2$), but with the extra condition, subject to some unchecked compatibilities, which have now been settled by Bryden Cais in [Cai07], Chapter 10. \square

In this article we give a somewhat different proof and remove the condition in the case $p = 2$. The main objective, however, is to extend the representation $\overline{\rho}_g$ to a 2-dimensional Galois representation with coefficients in the weight 1 Hecke algebra and to show, in most cases, that it is also unramified outside N , in particular at p , with the natural characteristic polynomials at all unramified primes.

We now introduce the notation necessary to state the main result. Let $S_1(\Gamma_1(N); \overline{\mathbb{F}}_p)_{\text{Katz}}$ be the $\overline{\mathbb{F}}_p$ -vector space of cuspidal Katz modular forms of weight 1 on $\Gamma_1(N)$ over $\overline{\mathbb{F}}_p$ and let \mathbb{T}_1 be the Hecke algebra acting on it, i.e. the \mathbb{F}_p -subalgebra inside $\text{End}_{\overline{\mathbb{F}}_p}(S_1(\Gamma_1(N); \overline{\mathbb{F}}_p)_{\text{Katz}})$ generated by all Hecke operators T_n for $n \in \mathbb{N}$ (see also Section 2). Let \mathfrak{m} be the maximal ideal of \mathbb{T}_1 defined as the kernel of the ring homomorphism $\mathbb{T}_1 \xrightarrow{T_n \mapsto a_n} \overline{\mathbb{F}}_p$. Let $\mathbb{T}_{1,\mathfrak{m}}$ denote the localisation of \mathbb{T}_1 at \mathfrak{m} . For the representation $\overline{\rho}_g$ we shall also write $\overline{\rho}_{\mathfrak{m}}$.

Theorem 1.2. *Assume that $\overline{\rho}_{\mathfrak{m}}$ is irreducible and is not unramified at p with scalar $\overline{\rho}_{\mathfrak{m}}(\text{Frob}_p)$. Then there is a Galois representation*

$$\rho_{\mathfrak{m}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{T}_{1,\mathfrak{m}})$$

which is unramified outside N and such that for all primes $\ell \nmid N$ (including $\ell = p$) the characteristic polynomial of $\rho_{\mathfrak{m}}(\text{Frob}_{\ell})$ is $X^2 - T_{\ell}X + \langle \ell \rangle \in \mathbb{T}_{1,\mathfrak{m}}[X]$.

We include the following obvious corollary, which removes the condition in the case $p = 2$ from Proposition 1.1.

Corollary 1.3. *The representation $\overline{\rho}_g$ is unramified outside N and the characteristic polynomial of $\overline{\rho}_g(\text{Frob}_{\ell})$ equals $X^2 - a_{\ell}X + \epsilon(\ell)$ for all primes $\ell \nmid N$, including $\ell = p$.*

Proof. If $\overline{\rho}_{\mathfrak{m}} = \overline{\rho}_g$ is reducible, then it is automatically unramified at p as it is semisimple. If $\overline{\rho}_{\mathfrak{m}}$ is irreducible, the result follows by reducing $\rho_{\mathfrak{m}}$ (from Theorem 1.2) modulo \mathfrak{m} . \square

The proof of Theorem 1.2 will be given in Section 4 and we will illustrate the theorem with examples in Section 5. The essential point that makes the proof work is that cusp forms of weight 1 over $\overline{\mathbb{F}}_p$ sit in weight p in two different ways; on q -expansions the situation is precisely the same as in the theory of oldforms, when passing from level N to level Np . Let us call this ‘doubling’. We shall see that it leads to a ‘doubling of Hecke algebras’ and finally to a ‘doubling of Galois representations’. It is from the latter that we deduce the main statement.

In the proof of Theorem 1.2 we use essentially that $\overline{\rho}_{\mathfrak{m}}$ satisfies multiplicity one (see Section 3); hence, the case when $\overline{\rho}_{\mathfrak{m}}$ is unramified at p with scalar $\overline{\rho}_{\mathfrak{m}}(\text{Frob}_p)$, where multiplicity one fails by

Corollary 4.5 of [Wie07], has to remain open here. Moreover, in this article we also do not deal with the natural question whether $\mathbb{T}_{1,m}$ is actually a universal deformation ring of $\bar{\rho}_m$. We intend to investigate these questions and generalisations of the main results in future work.

Acknowledgements

I would like to thank Mladen Dimitrov for clarifying discussions and Jean-Pierre Serre for comments and hints on analysing the examples.

2 Modular forms and Hecke algebras of weight one

In this section we provide the statements on modular forms and Hecke algebras that are needed for the sequel. In particular, we deduce a ‘doubling of Hecke algebras’ from a ‘doubling of modular forms’.

We shall use the following notation and assumptions throughout the article.

Notation 2.1. • *Let p be a prime number and $N \geq 5$ an integer not divisible by p .*

- *Frob_ℓ always denotes an arithmetic Frobenius element at ℓ .*
- *ζ_n always denotes a primitive n -th root of unity (for $n \in \mathbb{N}$).*
- *If R is a ring, $S \subseteq R$ a subset and M an R -module, then we put $M[S] := \{m \in M \mid sm = 0\}$ and call it the S -kernel.*

Katz modular forms

For the treatment in this article, it is essential to dispose of the geometric definition of modular forms given by Katz. Since the tools we need are nicely exposed in [Edi06], we follow this article, and, in particular, we work with Katz modular cusp forms for the moduli problem $[\Gamma_1(N)]'_{\mathbb{F}_p}$ of elliptic curves with an embedding of the group scheme μ_N . We use the notation $S_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ for these. Replacing \mathbb{F}_p by a field extension \mathbb{F} of \mathbb{F}_p , one also defines $S_k(\Gamma_1(N); \mathbb{F})_{\text{Katz}}$. By flatness, $S_k(\Gamma_1(N); \mathbb{F})_{\text{Katz}} = \mathbb{F} \otimes_{\mathbb{F}_p} S_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$.

Let $\mathbb{T}_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ be the \mathbb{F}_p -subalgebra of $\text{End}_{\overline{\mathbb{F}_p}}(S_k(\Gamma_1(N); \overline{\mathbb{F}_p})_{\text{Katz}})$ generated by all Hecke operators T_n and let $\mathbb{T}'_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ be its subalgebra generated only by those T_n with $p \nmid n$. Note that both contain the diamond operators due to the formula $\ell^{k-1}\langle \ell \rangle = T_\ell^2 - T_{\ell^2}$ for a prime ℓ (use any two such ℓ that have the same reduction modulo N).

The q -expansion principle and the formula $a_1(T_n f) = a_n(f)$ provide the identification

$$\text{Hom}_{\mathbb{F}_p}(\mathbb{T}_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}, \mathbb{F}) \xrightarrow{\varphi \mapsto \sum_{n=1}^{\infty} \varphi(T_n) q^n} S_k(\Gamma_1(N); \mathbb{F})_{\text{Katz}} \quad (2.1)$$

for \mathbb{F}/\mathbb{F}_p .

Classical modular forms

It is useful to point out the relation with classical holomorphic cusp forms, for which we use the notation $S_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))_{\text{cl}}$. The corresponding Hecke algebra $\mathbb{T}_k(\Gamma_1(N))_{\text{cl}}$ is defined as the \mathbb{Z} -subalgebra of $\text{End}_{\mathbb{C}}(S_k(\Gamma_1(N))_{\text{cl}})$ generated by all Hecke operators T_n . By the existence of an integral structure and the q -expansion principle, the map $\text{Hom}_{\mathbb{Z}}(\mathbb{T}_k(\Gamma_1(N))_{\text{cl}}, \mathbb{C}) \rightarrow S_k(\Gamma_1(N))_{\text{cl}}$ which sends a map φ to the Fourier series $\sum_{n=1}^{\infty} \varphi(T_n) q^n$ with $q = q(z) = e^{2\pi iz}$ is an isomorphism. We let $S_k(\Gamma_1(N); R)_{\text{cl}} = \text{Hom}_{\mathbb{Z}}(\mathbb{T}_k(\Gamma_1(N))_{\text{cl}}, R)$ for any \mathbb{Z} -algebra R . Note $S_k(\Gamma_1(N); \mathbb{C})_{\text{cl}} = S_k(\Gamma_1(N))_{\text{cl}}$. Note also that due to the freeness and the finite generation of $\mathbb{T}_k(\Gamma_1(N))_{\text{cl}}$ as a \mathbb{Z} -module

$$R_2 \otimes_{R_1} S_k(\Gamma_1(N); R_1)_{\text{cl}} \cong S_k(\Gamma_1(N); R_2)_{\text{cl}} \quad (2.2)$$

for any R_1 -algebra R_2 .

The following proposition states that for weights at least 2, Katz cusp forms over $\overline{\mathbb{F}}_p$ coincide with reductions of classical ones of the same level $\Gamma_1(N)$.

Proposition 2.2. *Let $k \geq 2$. Assume $N \neq 1$ or $p \geq 5$.*

- (a) *There is an isomorphism $S_k(\Gamma_1(N); \mathbb{F})_{\text{cl}} \cong S_k(\Gamma_1(N); \mathbb{F})_{\text{Katz}}$ which is compatible with the Hecke operators and q -expansions for any \mathbb{F}/\mathbb{F}_p .*
- (b) *The map $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}_k(\Gamma_1(N))_{\text{cl}} \xrightarrow{1 \otimes T_n \mapsto T_n} \mathbb{T}_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ is an isomorphism of rings.*
- (c) *The map $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}'_k(\Gamma_1(N))_{\text{cl}} \xrightarrow{1 \otimes T_n \mapsto T_n} \mathbb{T}'_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ is an isomorphism of rings.*

Proof. (a) By [Edi06], 4.6, one has

$$\mathbb{F}_p \otimes_{\mathbb{Z}[\frac{1}{N}]} S_k(\Gamma_1(N); \mathbb{Z}[\frac{1}{N}])_{\text{Katz}} \cong S_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$$

compatible with the Hecke operators. By loc. cit. 4.7 one also has

$$S_k(\Gamma_1(N); \mathbb{Z}[\frac{1}{N}])_{\text{Katz}} \cong S_k(\Gamma_1(N); \mathbb{Z}[\frac{1}{N}])_{\text{cl}}.$$

Both identifications respect q -expansions. Invoking them together with Equation (2.2) gives the statement.

(b) From (a) it follows that $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}_k(\Gamma_1(N))_{\text{cl}} \xrightarrow{1 \otimes T_n \mapsto T_n} \mathbb{T}_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ is a surjection of rings. To see it is an isomorphism it suffices to invoke Equations (2.1) and (2.2) to give:

$$\begin{aligned} \text{Hom}_{\mathbb{F}_p}(\mathbb{T}_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}, \mathbb{F}_p) &\cong S_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}} \stackrel{(a)}{\cong} \\ &S_k(\Gamma_1(N); \mathbb{F}_p)_{\text{cl}} \cong \text{Hom}_{\mathbb{Z}}(\mathbb{T}_k(\Gamma_1(N))_{\text{cl}}, \mathbb{F}_p) \cong \text{Hom}_{\mathbb{F}_p}(\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}_k(\Gamma_1(N))_{\text{cl}}, \mathbb{F}_p), \end{aligned}$$

which is the map induced from $1 \otimes T_n \mapsto T_n$ due to the compatibility of q -expansions.

(c) This can be shown precisely as (b): From (a) it also follows that

$$\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}'_k(\Gamma_1(N))_{\text{cl}} \xrightarrow{1 \otimes T_n \mapsto T_n} \mathbb{T}'_k(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$$

is a surjection of rings. It is an isomorphism because the map

$$\mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}'_k(\Gamma_1(N); \mathbb{F}_p)_{\mathrm{Katz}}, \mathbb{F}_p) \rightarrow \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}'_k(\Gamma_1(N))_{\mathrm{cl}}, \mathbb{F}_p)$$

induced from $T_n \otimes 1 \mapsto T_n$ is an isomorphism. That is the case, since the left hand side can be identified with

$$\left\{ \sum_{n=1, p \nmid n}^{\infty} a_n q^n \in \mathbb{F}_p[[q]] \mid \exists f \in S_k(\Gamma_1(N); \mathbb{F}_p)_{\mathrm{Katz}} \text{ with } a_n(f) = a_n \forall n \text{ s.t. } p \nmid n \right\}$$

and the right hand side with the similarly defined space for $S_k(\Gamma_1(N); \mathbb{F}_p)_{\mathrm{cl}}$, so that we can conclude using (a). \square

Note that the corresponding statement for weight $k = 1$ is false. We shall explain examples in Section 5. That failure is actually *la raison d'être* of this article.

Doubling of weight one forms

Towards the goal of this article, the construction and study of a Galois representation into the weight 1 Hecke algebra, it is necessary to increase the weight, since weight 1 is not a cohomological weight. The increased weight will enable us to see the Galois representation on the Jacobian of a modular curve, thus, permitting the use of geometric tools.

We shall map weight 1 forms into weight p . This can be done in two different ways: multiplying by the Hasse invariant A (a modular form over \mathbb{F}_p of weight $p - 1$ with q -expansion 1); the Frobenius $F(f) = f^p$. The former does not change the q -expansion and the latter maps $\sum_{n=1}^{\infty} a_n q^n$ to $\sum_{n=1}^{\infty} a_n q^{np}$. Note that on the level of q -expansions, these two maps correspond precisely to the two degeneracy maps from level N to Np . Hence, weight one forms in weight p are very analogous to oldforms. That is the price to pay for the use of geometric tools.

Let \mathbb{F}/\mathbb{F}_p and consider the map

$$\Psi : (S_1(\Gamma_1(N); \mathbb{F})_{\mathrm{Katz}})^{\oplus 2} \rightarrow S_p(\Gamma_1(N); \mathbb{F})_{\mathrm{Katz}}, \quad (f, g) \mapsto A(f) + F(g) = Af + g^p. \quad (2.3)$$

By Proposition 4.4 of [Edi06] this is an injection. We shall write T_p for the Hecke operator in weight 1 and U_p for the one in weight p . According to Equation (4.2) of loc. cit. one has

$$\langle a \rangle \circ \Psi = \Psi \circ \begin{pmatrix} \langle a \rangle & 0 \\ 0 & \langle a \rangle \end{pmatrix}, \quad T_n \circ \Psi = \Psi \circ \begin{pmatrix} T_n & 0 \\ 0 & T_n \end{pmatrix}, \quad U_p \circ \Psi = \Psi \circ \begin{pmatrix} T_p & \mathrm{id} \\ -\langle p \rangle & 0 \end{pmatrix} \quad (2.4)$$

for $p \nmid n$ and $a \in \mathbb{Z}/N\mathbb{Z}^\times$.

The weight one Hecke algebra and doubling of Hecke algebras

From now on we use the abbreviations \mathbb{T}_k and \mathbb{T}'_k for $\mathbb{T}_k(\Gamma_1(N); \mathbb{F}_p)_{\mathrm{Katz}}$ and $\mathbb{T}'_k(\Gamma_1(N); \mathbb{F}_p)_{\mathrm{Katz}}$, respectively. Note that Equation (2.4) implies that \mathbb{T}'_p acts on $S_1(\Gamma_1(N); \mathbb{F})_{\mathrm{Katz}}$. In particular, mapping $T_n \mapsto T_n$ for $p \nmid n$ defines a ring surjection $\mathbb{T}'_p \twoheadrightarrow \mathbb{T}'_1$. Define

$$I := \mathbb{T}'_p \cap U_p \mathbb{T}'_p,$$

where the intersection is taken inside \mathbb{T}_p . We shall see in Corollary 2.6 (c) that I is the kernel of the previous surjection.

Lemma 2.3. (a) Inside $S_p(\Gamma_1(N); \mathbb{F})_{\text{Katz}}$ the equality $\text{Hom}_{\mathbb{F}_p}(\mathbb{T}_p, \mathbb{F})[\mathbb{T}'_p] = FS_1(\Gamma_1(N); \mathbb{F})_{\text{Katz}}$ holds (via Equation (2.1)).

(b) Inside $S_p(\Gamma_1(N); \mathbb{F})_{\text{Katz}}$ the equality $U_p \text{Hom}_{\mathbb{F}_p}(\mathbb{T}_p, \mathbb{F})[\mathbb{T}'_p] = AS_1(\Gamma_1(N); \mathbb{F})_{\text{Katz}}$ holds (via Equation (2.1)).

Proof. (a) The left hand side is equal to $\{f \in S_p(\Gamma_1(N); \mathbb{F})_{\text{Katz}} \mid a_n(f) = 0 \ \forall n \text{ s.t. } p \nmid n\}$. As this is precisely the kernel of Θ defined in [Kat77], part (3) of the main theorem of loc. cit. implies that it is equal to $FS_1(\Gamma_1(N); \mathbb{F})_{\text{Katz}}$. (b) follows from Equation (2.4), namely one has $U_p F = A$. \square

Proposition 2.4. (a) Let $f \in S_1(\Gamma_1(N); \mathbb{F})_{\text{Katz}}$ satisfy $a_n(f) = 0$ whenever $p \nmid n$. Then $f = 0$.

(b) $\mathbb{T}'_1 = \mathbb{T}_1$.

(c) $\mathbb{T}_p = \mathbb{T}'_p + U_p \mathbb{T}'_p$ as \mathbb{T}'_p -modules.

(d) There are $T, D \in \mathbb{T}'_p$ such that $U_p^2 - TU_p + D = 0$ in \mathbb{T}_p .

(e) I is an ideal of \mathbb{T}_p .

Proof. (a) The theorem of [Kat77] already used in the previous proof gives a contradiction for $f \neq 0$, since that f is in the kernel of Θ and has weight 1, so that it would have to come from an even smaller weight under Frobenius, which is impossible.

(b) If $\mathbb{T}_1/\mathbb{T}'_1$ were nonzero, then $S_1(\Gamma_1(N); \mathbb{F}_p)[\mathbb{T}'_1]$ would be nonzero and, hence, there would be a nonzero form $f \in S_1(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ such that $a_n(f) = 0$ whenever $p \nmid n$. This is, however, excluded by (a).

(c) Let $g \in S_p(\Gamma_1(N); \overline{\mathbb{F}}_p)[\mathbb{T}'_p + U_p \mathbb{T}'_p]$. Now g satisfies $a_n(g) = 0$ whenever $p^2 \nmid n$. Thus, there is $f \in S_1(\Gamma_1(N); \overline{\mathbb{F}}_p)_{\text{Katz}}$ such that $Ff = g$ (again by [Kat77]) satisfying $a_n(f) = 0$ whenever $p \nmid n$, so that by (a) it is zero, implying the claim.

(d) This is immediate from (c).

(e) Let $x \in \mathbb{T}'_p \cap U_p \mathbb{T}'_p$. Thus, there is $y \in \mathbb{T}'_p$ such that $x = U_p y$. We have

$$U_p x = U_p^2 y = TU_p y - Dy = Tx - Dy \in \mathbb{T}'_p,$$

whence $U_p x \in I$. \square

Let \mathfrak{m}' be a maximal ideal of \mathbb{T}'_p . By $\mathbb{T}_{p, \mathfrak{m}'}$ and $\mathbb{T}'_{p, \mathfrak{m}'}$ we denote localisation at \mathfrak{m}' . We also use similar notation in similar circumstances.

Lemma 2.5. Let \mathfrak{m}' be a maximal ideal of \mathbb{T}'_p .

(a) The following statements are equivalent:

- (i) $\mathbb{T}'_{p,m'} \neq \mathbb{T}_{p,m'}$.
- (ii) *There is a normalised eigenform $g \in S_1(\Gamma_1(N); \overline{\mathbb{F}}_p)_{\text{Katz}}$ with q -expansion $\sum_{n=1}^{\infty} a_n q^n$ such that the map $\mathbb{T}'_p \xrightarrow{T_n \mapsto a_n} \overline{\mathbb{F}}_p$ defines a ring homomorphism with kernel \mathfrak{m}' .*

If the equivalent statements hold, then we say that \mathfrak{m}' comes from weight 1.

- (b) *We have $\mathbb{T}_{p,m'} \cong \prod_{i=1}^n \mathbb{T}_{p,\tilde{\mathfrak{m}}_i}$ with $n \in \{1, 2\}$, where the $\tilde{\mathfrak{m}}_i$ are the maximal ideals of \mathbb{T}_p containing \mathfrak{m}' .*

If one of the $\tilde{\mathfrak{m}}_i$ is ordinary (meaning that $U_p \in \mathbb{T}_{p,\tilde{\mathfrak{m}}_i}^\times$), then all are and we say that \mathfrak{m}' is ordinary.

Suppose now that \mathfrak{m}' comes from weight one with $g \in S_1(\Gamma_1(N); \overline{\mathbb{F}}_p)_{\text{Katz}}$ as in (a). Then \mathfrak{m}' is ordinary. Furthermore, $n = 2$ if and only if $a_p^2 \neq 4\epsilon(p)$, where ϵ is the Dirichlet character of g . In that case we say that \mathfrak{m}' is p -distinguished.

Proof. (a) Statement (ai) means that $U_p \in \mathbb{T}_{p,m'}$ is not in $\mathbb{T}'_{p,m'}$, i.e. that $\mathbb{T}_{p,m'}/\mathbb{T}'_{p,m'} \neq 0$ and, equivalently, $\mathbb{T}_{p,m'}^\vee[\mathbb{T}'_{p,m'}] \cong S_p(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz},m'}[\mathbb{T}'_{p,m'}] \neq 0$. This, however, is equivalent to the existence of a cusp form $f \in S_p(\Gamma_1(N); \overline{\mathbb{F}}_p)_{\text{Katz}}$ such that $a_n(f) = 0$ for all $p \nmid n$ and such that it is an eigenfunction for all T_n with $p \nmid n$. By the theorem of [Kat77] used already in the proof of Lemma 2.3, any such is of the form $f = Fh$ with $h \in S_1(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$. Hence, there is a normalised eigenform $g \in S_1(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ such that the $a_n(g)$ are the eigenvalues of T_n on f for $p \nmid n$, whence (aii).

Conversely, the existence of g implies that $S_p(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz},m'}[\mathbb{T}'_{p,m'}] \neq 0$, as it contains Fg , so that $\mathbb{T}'_{p,m'} \neq \mathbb{T}_{p,m'}$.

(b) The product decomposition into its localisations is a general fact of Artinian rings. If $\mathbb{T}'_{p,m'} = \mathbb{T}_{p,m'}$, there is nothing to show. So we assume now that this equality does not hold. From Proposition 2.4 (d) we have the surjection of rings

$$\mathbb{T}'_{p,m'}[X]/(X^2 - TX + D) \xrightarrow{X \mapsto U_p} \mathbb{T}_{p,m'}.$$

Taking it mod \mathfrak{m}' yields $\mathbb{F}[X]/(X^2 - \bar{T}X + \bar{D})$ on the left hand side with $\mathbb{F} = \mathbb{T}'_p/\mathfrak{m}'$, which has at most two local factors, depending on whether the quadratic equation has two distinct roots or a double one. Thus there can at most be two local factors on the right hand side. Modulo \mathfrak{m}' , the quadratic polynomial is in fact $X^2 - a_p(g)X + \epsilon(p)$, which follows from the explicit shape of U_p given in Equation (2.4); see also Corollary 2.6 (a). The ordinarity is now also clear since $\epsilon(p)$ is non-zero in \mathbb{F} . \square

We assume henceforth that \mathfrak{m}' comes from weight 1 and is hence ordinary. We write $\Psi_{\mathfrak{m}'}$ for the localisation of Ψ (from Equation (2.3)) at \mathfrak{m}' and similarly $I_{\mathfrak{m}'} = \mathbb{T}'_{p,m'} \cap U_p \mathbb{T}'_{p,m'}$.

Corollary 2.6. *Let \mathfrak{m}' be a maximal ideal of \mathbb{T}'_p which comes from weight 1.*

- (a) *We have $(S_1(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz},m'})^{\oplus 2} \xrightarrow{\Psi_{\mathfrak{m}'}} S_p(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz},m'}[I_{\mathfrak{m}'}]$. The operator U_p acts on the left hand side as $\begin{pmatrix} T_p & 1 \\ -\langle p \rangle & 0 \end{pmatrix}$. The operator T_n for $p \nmid n$ acts as $\begin{pmatrix} T_n & 0 \\ 0 & T_n \end{pmatrix}$.*

(b) There is a natural isomorphism $\mathbb{T}_{p,m'}/I_{m'} \cong \mathbb{T}_{1,m'} \oplus \mathbb{T}_{1,m'}$ of $\mathbb{T}'_{p,m'}$ -modules. The operator U_p acts on the right hand side as $\begin{pmatrix} T_p & -\langle p \rangle \\ 1 & 0 \end{pmatrix}$. The operator T_n for $p \nmid n$ acts as $\begin{pmatrix} T_n & 0 \\ 0 & T_n \end{pmatrix}$.

(c) The ring homomorphism $\mathbb{T}'_{p,m'} \xrightarrow{T_n \mapsto T_n} \mathbb{T}_{1,m'}$ is surjective with kernel $I_{m'}$.

Proof. (a) By Lemma 2.5, U_p is invertible and by Proposition 2.4 (e), $I_{m'}$ is an ideal of $\mathbb{T}_{p,m'}$. Thus, we have $I_{m'} = U_p^{-1} I_{m'} = \mathbb{T}'_{p,m'} \cap U_p^{-1} \mathbb{T}'_{p,m'}$. It follows that

$$\begin{aligned} \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}, \mathbb{F})[I_{m'}] &\cong \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}, \mathbb{F})[\mathbb{T}'_{p,m'}] \oplus \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}, \mathbb{F})[U_p^{-1} \mathbb{T}'_{p,m'}] \\ &= \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}, \mathbb{F})[\mathbb{T}'_{p,m'}] \oplus U_p \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}, \mathbb{F})[\mathbb{T}'_{p,m'}] \\ &\cong A(S_1(\Gamma_1(N))_{\mathrm{Katz}})_{m'} \oplus F(S_1(\Gamma_1(N))_{\mathrm{Katz}})_{m'} = \mathrm{im}(\Psi_{m'}), \end{aligned}$$

using Lemma 2.3. Moreover, Equation (2.1) gives an isomorphism $S_p(\Gamma_1(N); \mathbb{F}_p)_{\mathrm{Katz}, m'}[I_{m'}] \cong \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}, \mathbb{F})[I_{m'}]$. The shapes of U_p and T_n are taken from Equation (2.4).

(b) Using Equation (2.1), (a) can be reformulated as an isomorphism

$$\mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}/I_{m'}, \mathbb{F}_p) \cong \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}, \mathbb{F}_p)[I_{m'}] \cong \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{1,m'}, \mathbb{F}_p)^{\oplus 2}.$$

Dualising it yields the statement, and the matrices are just the transposes of the matrices in the previous part.

(c) The algebra generated by the T_n with $p \nmid n$ on the left hand side of (b) is $\mathbb{T}'_{p,m'}/I_{m'}$ and on the right hand side $\mathbb{T}'_{1,m'}$, which equals $\mathbb{T}_{1,m'}$ by Proposition 2.4 (b). \square

We refer to (b) as ‘doubling of Hecke algebras’. Part (c) is the key for the definition of the Galois representation with coefficients in $\mathbb{T}_{1,m'}$.

Passage to weight two

In order to work on the Jacobian of a modular curve, we pass from weight p to weight 2, which is only necessary if $p > 2$. We assume this for this subsection.

Proposition 2.7. *Let $N \geq 5$, $p \nmid N$, $p > 2$ and $\tilde{\mathfrak{m}}$ an ordinary maximal ideal of $\mathbb{T}_p(\Gamma_1(N); \mathbb{F}_p)_{\mathrm{Katz}}$. Then there is a unique maximal ideal \mathfrak{m}_2 of $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}_2(\Gamma_1(Np))_{\mathrm{cl}}$ such that $T_n \mapsto T_n$ for all n defines a ring isomorphism $\mathbb{T}_p(\Gamma_1(N); \mathbb{F}_p)_{\mathrm{Katz}, \tilde{\mathfrak{m}}} \cong (\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}_2(\Gamma_1(Np))_{\mathrm{cl}})_{\mathfrak{m}_2}$.*

Proof. This is due to Hida and follows, for instance, from combining Proposition 2.2 and [KW08], Proposition 2.3. \square

Remembering $\mathbb{T}_{p,m'} = \prod_{i=1}^n \mathbb{T}_{p,\tilde{\mathfrak{m}}_i}$ (see Lemma 2.5), we obtain that after localisation at ordinary m' , the Hecke algebra $\mathbb{T}_{p,m'}$ acts on the p -torsion of the Jacobian of $X_1(Np)$. We shall henceforth use this action without specifying the isomorphism from Proposition 2.7 explicitly.

3 The Galois representation of weight one

In this section we shall construct the Galois representation $\rho_{\mathfrak{m}}$, identify it on the Jacobian of a suitable modular curve and derive that it ‘doubles’ from the ‘doubling of Hecke algebras’.

We collect some statements and pieces of notation which are in place for the whole of this section.

Notation 3.1. *Next to Notation 2.1 we use the following pieces of notation and the following assumptions.*

- $\mathbb{T}_p = \mathbb{T}_p(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ denotes the full Hecke algebra on $S_p(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ and \mathbb{T}'_p is its subalgebra generated by those T_n with $p \nmid n$. The p -th Hecke operator is denoted U_p .
- \mathbb{T}_1 is the Hecke algebra on $S_1(\Gamma_1(N); \mathbb{F}_p)_{\text{Katz}}$ and it is equal to \mathbb{T}'_1 (see Proposition 2.4). The p -th Hecke operator is denoted T_p .
- The map $\mathbb{T}'_p \xrightarrow{T_n \mapsto T_n} \mathbb{T}_1$ defines a ring surjection with kernel $I = \mathbb{T}'_p \cap U_p \mathbb{T}'_p$ (see Corollary 2.6 (c)).
- Let \mathfrak{m}' be a maximal ideal of \mathbb{T}'_p which comes from weight 1 and corresponds to a normalised eigenform $g \in S_1(\Gamma_1(N); \overline{\mathbb{F}}_p)_{\text{Katz}}$ (see Lemma 2.5). Let ϵ be the Dirichlet character of g . Then \mathfrak{m}' is ordinary (see Lemma 2.5). Denote by \mathfrak{m} the maximal ideal of \mathbb{T}_1 the preimage of which in \mathbb{T}'_p is \mathfrak{m}' , whence $\mathbb{T}'_p/\mathfrak{m}' = \mathbb{T}_1/\mathfrak{m}$. Then \mathfrak{m} corresponds to the $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ -conjugacy class of g , i.e. it is the kernel of the ring homomorphism $\mathbb{T}_1 \xrightarrow{T_n \mapsto a_n(g)} \overline{\mathbb{F}}_p$.
- Either $\mathbb{T}_{p, \mathfrak{m}'} \cong \mathbb{T}_{p, \tilde{\mathfrak{m}}_1} \times \mathbb{T}_{p, \tilde{\mathfrak{m}}_2}$ (the p -distinguished case), or $\mathbb{T}_{p, \mathfrak{m}'}$ is local (see Lemma 2.5).

Existence

By work of Shimura and Deligne there is a Galois representation

$$\bar{\rho}_{\mathfrak{m}} = \bar{\rho}_{\mathfrak{m}'} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{T}_1/\mathfrak{m}) = \text{GL}_2(\mathbb{T}'_p/\mathfrak{m}')$$

characterised by the property that it is unramified outside Np and

$$\text{charpoly}(\bar{\rho}_{\mathfrak{m}})(\text{Frob}_{\ell}) = X^2 - T_{\ell}X + \langle \ell \rangle \in \mathbb{T}_1/\mathfrak{m} \cong \mathbb{T}'_p/\mathfrak{m}'$$

for all primes $\ell \nmid Np$. Under the assumption that $\bar{\rho}_{\mathfrak{m}}$ is absolutely irreducible, Carayol in [Car94], Théorème 3, shows the existence of a Galois representation

$$\rho_{\mathfrak{m}'} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{T}'_{p, \mathfrak{m}'})$$

characterised by the property that it is unramified outside Np and $\text{charpoly}(\rho_{\mathfrak{m}'}(\text{Frob}_{\ell})) = X^2 - T_{\ell}X + \langle \ell \rangle \in \mathbb{T}'_{p, \mathfrak{m}'}$ for all primes $\ell \nmid Np$. In fact, the reference gives a twist of this representation. Later on, we are going to be more precise about which twist it is. As a general rule, we denote $\bar{\rho}$ a representation with coefficients in a finite field or $\overline{\mathbb{F}}_p$ and ρ when the coefficients are in a Hecke algebra.

Proposition 3.2. *Let \mathfrak{m} be a maximal ideal of \mathbb{T}_1 such that $\bar{\rho}_{\mathfrak{m}}$ is absolutely irreducible. Then there is a Galois representation*

$$\rho_{\mathfrak{m}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{T}_{1,\mathfrak{m}})$$

characterised by the property that it is unramified outside Np and $\text{charpoly}(\rho_{\mathfrak{m}}(\text{Frob}_{\ell})) = X^2 - T_{\ell}X + \langle \ell \rangle \in \mathbb{T}_{1,\mathfrak{m}}$ for all primes $\ell \nmid Np$.

Proof. It suffices to compose $\rho_{\mathfrak{m}'}$ with $\text{GL}_2(\mathbb{T}'_{p,\mathfrak{m}'}) \rightarrow \text{GL}_2(\mathbb{T}_{1,\mathfrak{m}})$ coming from Corollary 2.6 (c). \square

The p -divisible group for $p = 2$

Assume for the moment that $p = 2$. Let J be the Jacobian $J_1(N)$ of $X_1(N)$, which is defined over \mathbb{Q} . Let G be the \mathfrak{m}' -component of the p -divisible group $J[p^{\infty}]_{\mathbb{Q}}$ attached to J .

A word of explanation is necessary (see also [Gro90], Section 12). The maximal ideals $\tilde{\mathfrak{m}}$ of \mathbb{T}_p containing \mathfrak{m}' correspond under pull-back to unique maximal ideals of the Hecke algebra $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{T}_p(\Gamma_1(N))_{\text{cl}}$, using Proposition 2.2. This Hecke algebra acts on the Tate module of J and localisation at each $\tilde{\mathfrak{m}}$ gives a direct factor of it. Then G is the direct product of the (at most two by Lemma 2.5) corresponding p -divisible groups. If \mathfrak{m}' is p -distinguished, then we shall denote by G_1 and G_2 the two p -divisible groups such that $G = G_1 \times G_2$.

The p -divisible group for $p > 2$

Assume now $p > 2$. We proceed very similarly to the above: Let J be the Jacobian $J_1(Np)$ of $X_1(Np)$, which is defined over \mathbb{Q} . Let G be the \mathfrak{m}' -component of the p -divisible group $J[p^{\infty}]_{\mathbb{Q}}$ attached to J .

Here we use that the ideals $\tilde{\mathfrak{m}}$ of \mathbb{T}_p containing \mathfrak{m}' correspond to unique maximal ideals of the Hecke algebra $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}_2(\Gamma_1(Np))_{\text{cl}}$ by Proposition 2.7. In turn they give rise, by taking preimages, to unique maximal ideals of $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{T}_2(\Gamma_1(Np))_{\text{cl}}$. For each of these (at most two, by Lemma 2.5) maximal ideals we take the p -divisible group of the corresponding factor of the Tate module of J . Thus, if \mathfrak{m}' is p -distinguished, then G is of the form $G_1 \times G_2$.

Properties of the p -divisible group

We assume that G (and G_1 and G_2 in the p -distinguished case) is as defined above (for either $p = 2$ or $p > 2$).

Proposition 3.3. *The p -divisible group G acquires good reduction over $\mathbb{Z}_p[\zeta_p]$. Let G^0 and G^e be the connected component and the étale quotient of G over $\mathbb{Z}_p[\zeta_p]$, respectively.*

- (a) *The module $G^0[p](\overline{\mathbb{Q}}_p)$ is unramified over $\mathbb{Q}_p(\zeta_p)$ and there is an isomorphism $G^0[p](\overline{\mathbb{Q}}_p) \cong \mathbb{T}_{p,\mathfrak{m}'}$ of $\mathbb{T}_{p,\mathfrak{m}'}$ -modules, under which any arithmetic Frobenius $\text{Frob}_p \in \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p(\zeta_p))$ acts as U_p^{-1} .*

(b) The exact sequence $0 \rightarrow G^0 \rightarrow G \rightarrow G^e \rightarrow 0$ gives rise to the exact sequence

$$0 \rightarrow \mathbb{T}_{p,m'} \rightarrow G[p](\overline{\mathbb{Q}}_p) \rightarrow \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}, \mathbb{F}_p) \rightarrow 0$$

of $\mathbb{T}_{p,m'}$ -modules, under the identification of (a) and its dual.

Proof. This follows immediately from applying [Wie07], Proposition 2.2, Corollary 2.3 and Theorem 3.1 for all maximal ideals $\tilde{\mathfrak{m}} \subset \mathbb{T}_p$ containing \mathfrak{m}' . We stress that those results were all derived from [Gro90]. \square

Since in this article we are using arithmetic Frobenius elements, and on modular curves (with level structure of the type $\mu_N \hookrightarrow E[N]$) geometric ones are more natural, we have to twist our representations at various places.

It is well-known that $\overline{\rho}_{\mathfrak{m}} \otimes \epsilon^{-1}$ is contained in $G[p](\overline{\mathbb{Q}})[\mathfrak{m}']$ (possibly more than once, see e.g. [Wie07], Proposition 4.1).

The following theorem is the result of the work of many authors. We do not intend to give all the original references, but, content ourselves by referring to a place in the literature where the statements appear as we need them.

Theorem 3.4 (Mazur, Wiles, Gross, Ribet, Buzzard, Tilouine, Edixhoven, W.). *Assume that $\overline{\rho}_{\mathfrak{m}}$ is absolutely irreducible. Then the following statements are equivalent:*

- (i) $\overline{\rho}_{\mathfrak{m}}$ is unramified at p and $\overline{\rho}_{\mathfrak{m}}(\mathrm{Frob}_p)$ is non-scalar or $\overline{\rho}_{\mathfrak{m}}$ is ramified at p .
- (ii) $G[p](\overline{\mathbb{Q}})[\tilde{\mathfrak{m}}] \cong \overline{\rho}_{\mathfrak{m}}$ for any maximal ideal $\tilde{\mathfrak{m}} \subset \mathbb{T}_p$ containing \mathfrak{m}' , i.e. $\overline{\rho}_{\mathfrak{m}}$ satisfies multiplicity one on the Jacobian.
- (iii) $\mathbb{T}_{p,m'} \cong \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{T}_{p,m'}, \mathbb{F}_p)$, i.e. $\mathbb{T}_{p,m'}$ is Gorenstein.

If the equivalent statements hold, then $G[p](\overline{\mathbb{Q}}) \cong \mathbb{T}_{p,m'} \oplus \mathbb{T}_{p,m'}$.

Proof. For the implication (i) \Rightarrow (ii) we refer, for instance, to [KW08], Theorem 1.2. The implication (ii) \Rightarrow (i) is the content of [Wie07], Corollary 4.5. The equivalence of (ii) and (iii) is proved, for instance, in [KW08], Proposition 2.2 (b). That (ii) implies the final statement is, for example, proved in [KW08], Proposition 2.1. \square

Note that by Proposition 1.1 the case that $\overline{\rho}_{\mathfrak{m}}$ is ramified at p is known not to occur in almost all cases. We are proving in Corollary 1.3 that it actually never occurs.

The Galois representation on the Jacobian

We proceed under the following assumptions:

Assumption 3.5. *We continue to use Notation 2.1 and 3.1. Moreover:*

- $\bar{\rho}_m$ denotes the residual Galois representation introduced above. It is the residual representation attached to g . We assume that $\bar{\rho}_m$ is absolutely irreducible.
- Let G (and G_1, G_2 in the p -distinguished case) the p -divisible group introduced earlier.
- We assume that $\bar{\rho}_m$ satisfies multiplicity one on the Jacobian so that $G[p](\bar{\mathbb{Q}}) \cong \mathbb{T}_{p,m'} \oplus \mathbb{T}_{p,m'}$ (see Theorem 3.4).
- Let $\tilde{\epsilon} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \mathbb{Z}/(N)^\times \xrightarrow{a \mapsto \langle a \rangle} \mathbb{T}_p'^\times$. Note that composing $\tilde{\epsilon}$ with $\mathbb{T}_{p,m'}'^\times \rightarrow (\mathbb{T}_p'/\mathfrak{m}')^\times$ equals ϵ , the Dirichlet character of g , seen as a character of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The next proposition can be considered as a ‘doubling of Galois representations’.

Proposition 3.6. *We use Assumption 3.5. Let $\rho_{I_{m'}} := G[p](\bar{\mathbb{Q}}) \otimes_{\mathbb{T}_{p,m'}} \mathbb{T}_{1,m}$. Then there is an isomorphism*

$$\rho_{I_{m'}} \cong (\rho_m \otimes \tilde{\epsilon}^{-1}) \oplus (\rho_m \otimes \tilde{\epsilon}^{-1}).$$

of $\mathbb{T}_{1,m}[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ -modules.

Proof. From [Car94], 3.3.2, and Theorem 3.4 it follows that $H := G[p](\bar{\mathbb{Q}}) \cong \mathbb{T}_{p,m'} \oplus \mathbb{T}_{p,m'}$ as $\mathbb{T}_{p,m'}[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ -modules and that it is characterised by the property that it is unramified outside Np and that the characteristic polynomial of Frob_ℓ is $X^2 - T_\ell/\langle \ell \rangle X + 1/\langle \ell \rangle \in \mathbb{T}_{p,m'}'[X]$ for all primes $\ell \nmid Np$. We recall that [Car94] works with geometric Frobenius elements, whereas we are using arithmetic ones, accounting for the differences in the formulae.

By Théorème 2 of loc. cit., H is obtained by scalar extension of some $\mathbb{T}_{p,m'}'[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ -module $H' \cong \mathbb{T}_{p,m'}' \oplus \mathbb{T}_{p,m'}'$, i.e. $H = H' \otimes_{\mathbb{T}_{p,m'}'} \mathbb{T}_{p,m'}$. Note that in this description H is a $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ -module via an action on H' and a $\mathbb{T}_{p,m'}$ -module via the natural action on $\mathbb{T}_{p,m'}$ in the tensor product.

Next we have the following isomorphisms of $\mathbb{T}_{p,m'}'[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ -modules:

$$\begin{aligned} H \otimes_{\mathbb{T}_{p,m'}} \mathbb{T}_{p,m'}/I_{m'} &\cong (H' \otimes_{\mathbb{T}_{p,m'}'} \mathbb{T}_{p,m'}) \otimes_{\mathbb{T}_{p,m'}} \mathbb{T}_{p,m'}/I_{m'} \cong H' \otimes_{\mathbb{T}_{p,m'}'} \mathbb{T}_{p,m'}/I_{m'} \\ &\cong H' \otimes_{\mathbb{T}_{p,m'}'} (\mathbb{T}_{1,m} \oplus \mathbb{T}_{1,m}) \cong (H' \otimes_{\mathbb{T}_{p,m'}'} \mathbb{T}_{1,m}) \oplus (H' \otimes_{\mathbb{T}_{p,m'}'} \mathbb{T}_{1,m}), \end{aligned}$$

where we used Corollary 2.6 (b). Note that the $\mathbb{T}_{p,m'}'[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ -action factors through to give a $\mathbb{T}_{1,m}[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$ -action.

Recall that $\rho_m : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{T}_{p,m'}'/I_{m'}) \cong \text{GL}_2(\mathbb{T}_{1,m})$ is characterised by it being unramified outside Np and the characteristic polynomial of Frob_ℓ for $\ell \nmid Np$ being equal to $X^2 - T_\ell X + \langle \ell \rangle$. Hence, the characteristic polynomial of $(\rho_m \otimes \tilde{\epsilon}^{-1})(\text{Frob}_\ell)$ is $X^2 - T_\ell/\langle \ell \rangle X + 1/\langle \ell \rangle$. Since $H' \otimes_{\mathbb{T}_{p,m'}'} \mathbb{T}_{1,m}$ satisfies the same properties, it agrees with $\rho_m \otimes \tilde{\epsilon}^{-1}$ by [Car94], Théorème 1. \square

4 Proof of Theorem 1.2

In this section we prove Theorem 1.2. We deal with the case when m' is p -distinguished and the case when $\mathbb{T}_{p,m'}$ is local separately.

Let us first remark that $N \geq 5$ can be assumed without loss of generality as follows. One can increase the level at some unramified auxiliary prime $q \geq 5$, $q \neq p$ and apply the theorem in level Nq , yielding a Galois representation with coefficients in the weight 1 Hecke algebra for $\Gamma_1(Nq)$ which is unramified outside Nq . Since the Hecke algebra for $\Gamma_1(N)$ is a quotient of the one for $\Gamma_1(Nq)$, one obtains the desired Galois representation, which is hence also unramified outside Nq . Choosing a different auxiliary q , one sees that the Galois representation for $\Gamma_1(N)$ is unramified at the auxiliary prime.

No tame ramification

We first show that there cannot be any tame ramification.

Lemma 4.1. *Let \mathbb{T} be a finite dimensional local \mathbb{F} -algebra with maximal ideal \mathfrak{m} for a finite extension \mathbb{F}/\mathbb{F}_p . If $A \in \ker(\mathrm{GL}_n(\mathbb{T}) \rightarrow \mathrm{GL}_n(\mathbb{T}/\mathfrak{m}))$ is a matrix such that $A^{p-1} = 1$, then $A = 1$.*

Proof. There is a matrix M all of whose entries are in \mathfrak{m} such that $A = 1 + M$. Thus $A = A^{p^r} = (1 + M)^{p^r} = 1 + M^{p^r}$ for all $r \in \mathbb{N}$. As \mathfrak{m} is a nilpotent ideal and all entries of M^{p^r} lie in \mathfrak{m}^{p^r} , it follows that $M = 0$. \square

Proposition 4.2. *Let \mathbb{T} be a finite dimensional local \mathbb{F} -algebra with maximal ideal \mathfrak{m} for a finite extension \mathbb{F}/\mathbb{F}_p . Let C be a subgroup of $\mathbb{Z}/(p-1)$ and $\rho : C \rightarrow \mathrm{GL}_2(\mathbb{T})$ a representation such that the residual representation $\bar{\rho} : C \rightarrow \mathrm{GL}_2(\mathbb{T}/\mathfrak{m})$ is trivial. Then ρ is trivial.*

Proof. As $\bar{\rho}$ is trivial, ρ takes its values in $\ker(\mathrm{GL}_n(\mathbb{T}) \rightarrow \mathrm{GL}_n(\mathbb{T}/\mathfrak{m}))$. But, this group does not have any nontrivial element of order dividing $p-1$ by Lemma 4.1, whence ρ is the trivial representation. \square

Corollary 4.3. *Let \mathbb{T} be a finite dimensional local \mathbb{F} -algebra with maximal ideal \mathfrak{m} for a finite extension \mathbb{F}/\mathbb{F}_p . Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \rightarrow \mathrm{GL}_2(\mathbb{T})$ be a representation and let $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \rightarrow \mathrm{GL}_2(\mathbb{T}/\mathfrak{m})$ be its residual representation. Assume that the semisimplification of $\bar{\rho}$ is unramified and that the restriction of ρ to $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p(\zeta_p))$ is unramified.*

Then ρ is unramified.

Proof. As the semisimplification of $\bar{\rho}$ is unramified and the restriction of ρ to $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p(\zeta_p))$ is also unramified, it follows that $\bar{\rho}$ is unramified. Moreover, the image of the inertia group has to be a subgroup of $\mathbb{Z}/(p-1)$, whence it acts trivially by Proposition 4.2. \square

The p -distinguished case

Proof of Theorem 1.2 – the p -distinguished case. Note that the assumptions of Theorem 1.2 imply that Assumption 3.5 is satisfied due to Theorem 3.4. We now assume that \mathfrak{m}' is p -distinguished,

i.e. $\mathbb{T}_{p,m'} \cong \mathbb{T}_{p,\tilde{m}_1} \times \mathbb{T}_{p,\tilde{m}_2}$. Let $m_i \in \mathbb{F}_p[X]$ be the minimal polynomial of U_p^{-1} acting on $\mathbb{T}_{p,\tilde{m}_i}$. Then m_1 and m_2 are powers of coprime irreducible polynomials. We obtain

$$G[p](\overline{\mathbb{Q}})/I_{m'} = G_1[p](\overline{\mathbb{Q}})/I_{m'} \oplus G_2[p](\overline{\mathbb{Q}})/I_{m'}$$

and $G_i[p](\overline{\mathbb{Q}})/I_{m'}$ is characterised by the fact that $m_i(U_p^{-1})$ annihilates it. From Proposition 3.6 it follows that $G[p](\overline{\mathbb{Q}})/I_{m'}$ is isomorphic to $(\rho_m \otimes \tilde{\epsilon}^{-1}) \oplus (\rho_m \otimes \tilde{\epsilon}^{-1})$ as $\mathbb{T}_{1,m}[\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$ -modules. But, as such $G_1[p](\overline{\mathbb{Q}})/I_{m'} \cong G_2[p](\overline{\mathbb{Q}})/I_{m'}$, thus for both $i = 1, 2$ we have $\rho_m \otimes \tilde{\epsilon}^{-1} \cong G_i[p](\overline{\mathbb{Q}})/I_{m'}$.

We are now going to work locally and let $\mathcal{G} = \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}(\zeta_p))$ and \mathcal{I} its inertia group. By Proposition 3.3 (a) applied to G_i we obtain for $i = 1, 2$ that

$$G_i^0[p](\overline{\mathbb{Q}_p})/I_{m'} \hookrightarrow (G_i[p](\overline{\mathbb{Q}_p})/I_{m'})^{\mathcal{I}} \cong (\rho_m \otimes \tilde{\epsilon}^{-1})^{\mathcal{I}}$$

and that Frob_p on the left hand side acts through U_p^{-1} , whence the image of the map is annihilated by $m_i(\text{Frob}_p)$. As the polynomials m_1 and m_2 are coprime, $G^0[p](\overline{\mathbb{Q}_p})/I_{m'} \cong G_1^0[p](\overline{\mathbb{Q}_p})/I_{m'} \oplus G_2^0[p](\overline{\mathbb{Q}_p})/I_{m'}$ is a subrepresentation of $(\rho_m \otimes \tilde{\epsilon}^{-1})^{\mathcal{I}}$. Counting \mathbb{F}_p -dimensions, it follows that

$$G^0[p](\overline{\mathbb{Q}_p})/I_{m'} \cong (\rho_m \otimes \tilde{\epsilon}^{-1})^{\mathcal{I}} \cong \rho_m \otimes \tilde{\epsilon}^{-1}.$$

Consequently, ρ_m is unramified at p , using Corollary 4.3 and taking into account that the semisimplification of $\overline{\rho}_m$ is unramified at p . Moreover, again due to Proposition 3.3 (a) the characteristic polynomial of Frob_p on $\rho_m \otimes \tilde{\epsilon}^{-1}$ is the one of U_p^{-1} , which is $X^2 - T_p/\langle p \rangle X + 1/\langle p \rangle$ (see Corollary 2.6), so that the one of $\rho_m(\text{Frob}_p)$ is as claimed. \square

The local case

Proposition 4.4. *Let R be a local \mathbb{F}_p -algebra which is finite dimensional as an \mathbb{F}_p -vector space and let \mathfrak{m} be its maximal ideal. Put $\mathbb{F} = R/\mathfrak{m}$. Let \mathcal{G} be a group. Let M, N, Q be $R[\mathcal{G}]$ -modules which are free of rank 2 as R -modules and suppose we have an exact sequence*

$$0 \rightarrow N \xrightarrow{\alpha} M \oplus M \rightarrow Q \rightarrow 0$$

of $R[\mathcal{G}]$ -modules. Suppose further that $\overline{N} := R/\mathfrak{m} \otimes_R N$ is indecomposable as an $\mathbb{F}[\mathcal{G}]$ -module.

Then $N \cong M \cong Q$ as $R[\mathcal{G}]$ -modules.

Proof. Write $\overline{M} := R/\mathfrak{m} \otimes_R M$. Counting dimensions as \mathbb{F} -vector spaces it follows that the sequence

$$0 \rightarrow \overline{N} \xrightarrow{\overline{\alpha}} \overline{M} \oplus \overline{M} \rightarrow \overline{Q} \rightarrow 0$$

is an exact sequence of $\mathbb{F}[\mathcal{G}]$ -modules. Consider the composite map

$$\phi_i : N \xrightarrow{\alpha} M \oplus M \xrightarrow{\text{pr}_i} M$$

for $i = 1, 2$, where pr_i is the projection on the i -th summand. Note that the ϕ_i are homomorphisms of $R[\mathcal{G}]$ -modules. Tensor ϕ_i with R/\mathfrak{m} to obtain

$$\overline{\phi}_i : \overline{N} \xrightarrow{\overline{\alpha}} \overline{M} \oplus \overline{M} \xrightarrow{\overline{\text{pr}}_i} \overline{M}.$$

Note that the cases $\dim_{\mathbb{F}} \text{im}(\overline{\phi_i}) \leq 1$ for $i = 1, 2$ cannot occur: If one of the dimensions is 1 and the other 0 or if both are 0, then one has a contradiction to the injectivity of $\overline{\alpha}$. If both are 1, then $\overline{N} \cong \text{im}(\overline{\phi_1}) \oplus \text{im}(\overline{\phi_2})$ as $\mathbb{F}[\mathcal{G}]$ -modules, which contradicts the assumed indecomposability of \overline{N} . Hence, there is $i \in \{1, 2\}$ such that $\dim_{\mathbb{F}} \text{im}(\overline{\phi_i}) = 2$. Hence, $\overline{\phi_i}$ is an isomorphism $\overline{N} \rightarrow \overline{M}$. It follows that $\phi_i : N \rightarrow M$ is surjective. Indeed, tensoring the exact sequence $N \xrightarrow{\phi_i} M \rightarrow S \rightarrow 0$ over R with R/\mathfrak{m} , shows that $\overline{S} = R/\mathfrak{m} \otimes_R S = 0$, whence $S = 0$ by Nakayama's lemma. As N and M are finite sets, ϕ_i is an isomorphism of $R[\mathcal{G}]$ -modules. \square

Proof of Theorem 1.2 – the local case. Note that the assumptions of Theorem 1.2 imply that Assumption 3.5 is satisfied due to Theorem 3.4. We now assume that $\mathbb{T}_{p, \mathfrak{m}'}$ is local. We are going to deduce the statement from Proposition 4.4. For R we take $\mathbb{T}_{1, \mathfrak{m}}$ and we let $\mathcal{G} := \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p(\zeta_p))$. In Proposition 3.6 we have seen that $\rho_{I_{\mathfrak{m}'}}$ is isomorphic to $(\rho_{\mathfrak{m}} \otimes \tilde{\epsilon}^{-1}) \oplus (\rho_{\mathfrak{m}} \otimes \tilde{\epsilon}^{-1})$ as $R[\mathcal{G}]$ -modules and we take M to be $\rho_{\mathfrak{m}} \otimes \tilde{\epsilon}^{-1}$.

Next we reduce the exact sequence of Proposition 3.3 (b) modulo $I_{\mathfrak{m}'}$. Due to multiplicity one, it remains exact (since it is split as a sequence of $\mathbb{T}_{p, \mathfrak{m}'}$ -modules), whence we obtain an exact sequence of $R[\mathcal{G}]$ -modules

$$0 \rightarrow \tilde{\rho} \rightarrow \rho_{I_{\mathfrak{m}'}} \rightarrow G^e[p](\overline{\mathbb{Q}_p})/I_{\mathfrak{m}'} \rightarrow 0,$$

where $\tilde{\rho} = G^0[p](\overline{\mathbb{Q}_p})/I_{\mathfrak{m}'}$. By Proposition 3.3 (a) we know that $\tilde{\rho}$ is unramified as a \mathcal{G} -module and it is free of rank 2 over R . Moreover, any arithmetic Frobenius at p acts through multiplication by U_p^{-1} . Also $G^e[p](\overline{\mathbb{Q}_p})/I_{\mathfrak{m}'}$ is free of rank 2 as an R -module. Taking $\tilde{\rho}$ modulo \mathfrak{m} we obtain an indecomposable $R/\mathfrak{m}[\mathcal{G}]$ -module, where the indecomposability is due to the formula for U_p (see Corollary 2.6). Hence, we take N to be $\tilde{\rho}$, restricted to \mathcal{G} .

Thus, from Proposition 4.4 we obtain $\rho_{\mathfrak{m}} \otimes \tilde{\epsilon}^{-1} \cong \tilde{\rho}$ as $\mathbb{T}_{1, \mathfrak{m}}[\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p(\zeta_p))]$ -modules, and, in particular, that $\rho_{\mathfrak{m}}$ is unramified at p , using Corollary 4.3 and taking into account that the semisimplification of $\overline{\rho}_{\mathfrak{m}}$ is unramified at p . Moreover, again due to Proposition 3.3 (a) the characteristic polynomial of Frob_p on $\rho_{\mathfrak{m}} \otimes \tilde{\epsilon}^{-1}$ is the one of U_p^{-1} , which is $X^2 - T_p/\langle p \rangle X + 1/\langle p \rangle$ (see Corollary 2.6), so that the one of $\rho_{\mathfrak{m}}(\text{Frob}_p)$ is as claimed. \square

5 Examples

We illustrate Theorem 1.2 by two examples. They both appeared first in Mestre's appendix to [Edi06] and we work them out in our context.

Both examples are of the following shape. Let \mathbb{F} be a finite field of characteristic p and $\mathbb{T} := \mathbb{F}[\epsilon] := \mathbb{F}[X]/(X^2)$. Then we have the split exact sequence of groups:

$$0 \rightarrow \text{Mat}_2(\mathbb{F})^0 \xrightarrow{A \mapsto 1 + \epsilon A} \text{SL}_2(\mathbb{T}) \xrightarrow{\epsilon \mapsto 0} \text{SL}_2(\mathbb{F}) \rightarrow 1,$$

where $\text{Mat}_2(\mathbb{F})^0$ denotes the 2×2 -matrices of trace zero (considered here as an abelian group with respect to addition), on which $\text{SL}_2(\mathbb{F})$ acts by conjugation (i.e. it is the adjoint representation). If $p > 2$, then this representation is irreducible, if $p = 2$ it has non-trivial submodules.

Example $p = 2, N = 229$

In this case there is only one normalised eigenform $g \in S_1(\Gamma_1(N); \overline{\mathbb{F}}_2)_{\text{Katz}}$ and thus only a unique maximal ideal $\mathfrak{m} \subset \mathbb{T}_1$. For example using MAGMA ([BCP97]) and a package developed by the author (see Appendix B of [Edi06] for an old version), one computes that $\mathbb{T}_1 \cong \mathbb{F}_2[\epsilon]$ and that $\overline{\rho}_{\mathfrak{m}} = \overline{\rho}_g : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{SL}_2(\mathbb{F}_2) \cong S_3$. If $\ker(\overline{\rho}_g) = \text{Gal}(\overline{\mathbb{Q}}/K)$, then K is the Hilbert class field of $\mathbb{Q}(\sqrt{229})$. Let us call G the image of $\rho_{\mathfrak{m}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{SL}_2(\mathbb{T})$ coming from Theorem 1.2. It turns out that $G \cap \text{Mat}_2(\mathbb{F}_2)^0 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$ (with the intersection being taken with respect to the map $A \mapsto 1 + \epsilon A$) and that $G \cong S_4$. In fact, this example can be obtained by reducing ρ_f , where f is a holomorphic weight 1 cuspidal eigenform with ρ_f having projective image S_4 .

Hence, the fact that $\rho_{\mathfrak{m}}$ is unramified at 2, which follows from Theorem 1.2, can already be deduced from the theorem of Deligne and Serre.

Example $p = 2, N = 1429$

In this case there is a normalised eigenform $g \in S_1(\Gamma_1(N); \overline{\mathbb{F}}_2)_{\text{Katz}}$ such that the image of $\overline{\rho}_g$ is isomorphic to $\text{SL}_2(\mathbb{F}_8)$. As $\text{SL}_2(\mathbb{F}_8)$ is not a quotient of any finite subgroup of $\text{GL}_2(\mathbb{C})$, this implies, as noted by Mestre, that g is not the reduction of any holomorphic weight 1 eigenform. Let \mathfrak{m} be the maximal ideal of \mathbb{T}_1 corresponding to g . One computes that $\mathbb{T}_{1,\mathfrak{m}} \cong \mathbb{F}_8[\epsilon]$. If $\ker(\overline{\rho}_g) = \text{Gal}(\overline{\mathbb{Q}}/K)$, then K is a Galois extension of \mathbb{Q} with Galois group $\text{SL}_2(\mathbb{F}_8)$ which is unramified outside the prime 1429.

Now consider $\rho_{\mathfrak{m}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{SL}_2(\mathbb{T}_{1,\mathfrak{m}})$ from Theorem 1.2 and let L be the Galois extension of \mathbb{Q} such that $\text{Gal}(\overline{\mathbb{Q}}/L) \cong \ker(\rho_{\mathfrak{m}})$, which is unramified outside 1429. After checking many Frobenius traces it seems very likely that L is $K(\sqrt{1429})$ and, hence, that $G := \text{im}(\rho_{\mathfrak{m}}) \cong \text{SL}_2(\mathbb{F}_8) \times \mathbb{Z}/(2)$. Explicitly, $G \cap \text{Mat}_2(\mathbb{F}_2)^0 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$.

In this case it is clear that L is unramified at 2 without appealing to Theorem 1.2. However, the remarkable phenomenon is that this extension L/\mathbb{Q} is detected by weight one Katz forms through their Hecke algebras. This points in the direction that one should ask if $\mathbb{T}_{1,\mathfrak{m}}$ is in fact a universal deformation ring of $\overline{\rho}_{\mathfrak{m}}$ in the category of local \mathbb{F}_p -algebras with residue field $\mathbb{T}_1/\mathfrak{m}$ for the local conditions of being unramified at p and minimally ramified elsewhere.

References

- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [Cai07] Bryden R. Cais. *Correspondences, integral structures, and compatibilities in p -adic cohomology*. ProQuest LLC, Ann Arbor, MI, 2007. Thesis (Ph.D.)—University of Michigan.
- [Car94] Henri Carayol. Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet. In *p -adic monodromy and the Birch and Swinnerton-Dyer conjecture*

- (*Boston, MA, 1991*), volume 165 of *Contemp. Math.*, pages 213–237. Amer. Math. Soc., Providence, RI, 1994.
- [CV92] Robert F. Coleman and José Felipe Voloch. Companion forms and Kodaira-Spencer theory. *Invent. Math.*, 110(2):263–281, 1992.
 - [DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.
 - [Edi06] Bas Edixhoven. Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one. *J. Inst. Math. Jussieu*, 5(1):1–34, 2006. With appendix A (in French) by Jean-François Mestre and appendix B by Gabor Wiese.
 - [Gro90] Benedict H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. J.*, 61(2):445–517, 1990.
 - [Kat77] Nicholas M. Katz. A result on modular forms in characteristic p . In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 53–61. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.
 - [KW08] L. J. P. Kilford and Gabor Wiese. On the failure of the Gorenstein property for Hecke algebras of prime weight. *Experiment. Math.*, 17(1):37–52, 2008.
 - [Wie07] Gabor Wiese. Multiplicities of Galois representations of weight one. *Algebra Number Theory*, 1(1):67–85, 2007. With an appendix by Niko Naumann.

Gabor Wiese
 Universität Duisburg-Essen
 Institut für Experimentelle Mathematik
 Ellernstraße 29
 45326 Essen
 Germany
 E-mail: gabor.wiese@uni-due.de
 Web page: <http://maths.pratum.net/>